This listing of claims will replace all prior versions, and listings, of claims in the application.

Listing of Claims:

1. (Previously Presented) A method of restoring data of a key-server in communication with a communication network comprising:

providing the key-server for storing secure electronic keys, the key-server in communication with the communication network;

providing to at least a computer in communication with the communication network, a plurality of portable data storage devices each having stored thereon secure electronic key data relating to a single authorized user; and,

copying from each of the plurality of portable data storage devices for storage in the key-server, secure electronic key data relating to the single authorized user.

2. (Currently Amended) A method of restoring data of a key-server in communication with a communication network as defined in claim 1 wherein the step of copying comprises:

forming a secure communication session between at least one of the plurality of portable data storage devices and the key-server;

transferring the secure electronic key data via the secure communication session from the portable data storage device to the key-server; and,

storing the transferred secure electronic key data within memory means of the key-server ~~ey-server~~.

3. (Previously Presented) A method of restoring data of a key-server in communication with a communication network as defined in claim 2 wherein the plurality of portable data storage devices comprise all the secure electronic key data to be restored in the key-server.

4. (Previously Presented) A method of restoring data of a key-server in communication with a communication network as defined in claim 3 wherein the plurality of

portable data storage devices includes memory having stored therein secure electronic key data relating to each single authorized user of the communication network.

5. (Previously Presented) A method of restoring data of a key-server in communication with a communication network as defined in claim 2 wherein the portable data storage device includes a processor for ciphering data using the secure electronic key data stored therein and comprising:

providing cryptographic functions within the portable data storage device using the secure electronic key data stored therein.

6. (Previously Presented) A method of restoring data of a key-server in communication with a communication network as defined in claim 2 wherein the key-server includes a processor for ciphering data using the secure electronic key data stored therein and comprising:

providing cryptographic functions within the key-server using the secure electronic key data stored therein.

7. (Currently Amended) A method of restoring data of a key-server in communication with a communication network as defined in claim 6 comprising:

determining at least an available user information entry device from a plurality of known user information entry devices;

receiving unique user identification information via the at least an available user information entry device; and,

registering the received user identification information against security data for that user stored in the key-server;

wherein, when the user identification information is indicative of an authorized user ciphering of data is performed with secure electronic key data associated with the authorized user.

8. (Original) A method of restoring data of a key-server in communication with a communication network as defined in claim 3 wherein each of the plurality of portable data

storage devices are provided at each of a plurality of computers in communication with the network.

9. (Original) A method of restoring data of a key-server in communication with a communication network as defined in claim 8 wherein the portable data storage device is one of a token and a smart card.

10. (Original) A method of restoring data of a key-server in communication with a communication network as defined in claim 2 wherein the portable data storage device is one of a token and a smart card.

11. (Original) A method of restoring data of a key-server in communication with a communication network as defined in claim 2 wherein at least a portable data storage device provides dedicated cryptographic functions for the at least a computer in communication with the communication network using the security data stored internal to the at least a portable data storage device.

12. (Original) A method of restoring data of a key-server in communication with a communication network as defined in claim 11 wherein the security data stored internal to the at least a portable data storage device are not accessible in a useable form from outside of the key-server and the at least a portable data storage device.

13. (Original) A method of restoring data of a key-server in communication with a communication network as defined in claim 2 wherein the key-server provides dedicated cryptographic functions for the at least a computer in communication with the communication network using the security data stored internal to the key-server.

14. (Previously Presented) A method of backing up data of a key-server in communication with a communication network comprising:

providing the key-server in communication with the communication network, the key-server having stored thereon the unique user identification information for a plurality of authorized users of the communication network and the secure electronic key data for use by the specific authorized user in accessing data within the network;

providing to at least a computer in communication with the communication network, a portable data storage device;

receiving user identification data indicative of an authorized user of the communication network; and,

copying from the key-server to the portable data storage device, secure electronic key data relating to the authorized user for use by the specific authorized user in accessing data within the network.

15. (Previously Presented) A method of backing up data of a key-server in communication with a communication network as defined in claim 14 wherein copying comprises:

forming a secure communication session between the key-server and the portable data storage device;

transferring the secure electronic key data relating to a specific authorized user via the secure communication session from the key-server to the portable data storage device assigned to that specific authorized user; and,

storing the transferred secure electronic key data relating to a specific authorized user within memory means of the portable data storage device.

16. (Previously Presented) A method of backing up data of a key-server in communication with a communication network as defined in claim 15 wherein secure electronic key data specific to each of a plurality of authorized users of the communication network is stored on a separate portable data storage device assigned uniquely to one of the plurality of authorized users,

wherein the secure electronic key data of the key-server is partially stored within each portable data storage device and wherein all data within the plurality of portable data storage devices is sufficient to restore security data to the key-server in the event of a data loss thereto.

17. (Previously Presented) A method of backing up data of a key-server in communication with a communication network as defined in claim 15 wherein the portable data storage device includes a processor for ciphering data using the secure electronic key data stored therein and comprising:

providing cryptographic functions within the portable data storage device using the secure electronic key data stored therein.

18. (Previously Presented) A method of backing up data of a key-server in communication with a communication network as defined in claim 15 wherein the key-server includes a processor for ciphering data using the secure electronic key data stored therein and comprising:

providing cryptographic functions within the key-server using the secure electronic key data stored therein.

19. (Currently Amended) A method of backing up data of a key-server in communication with a communication network as defined in claim 18 comprising:

determining at least an available user information entry device from a plurality of known user information entry devices;

receiving unique user identification information via the at least an available user information entry device; and,

registering the received user identification information against secure electronic ~~lectronic~~ key data for that user stored in the key-server,

wherein, when the user identification information is indicative of an authorized user, ciphering of data is performed with secure electronic key data associated with the authorized user.

20. (Original) A method of backing up data of a key-server in communication with a communication network as defined in claim 16 wherein each of the plurality of portable data storage devices are provided at each of a plurality of computers in communication with the network.

21. (Previously Presented) A method of backing up data of a key-server in communication with a communication network as defined in claim 20 wherein the portable storage device comprises an interface.

22. (Previously Presented) A method of backing up data of a key-server in communication with a communication network as defined in claim 16 wherein the portable storage device comprises an interface.

23. (Previously Presented) A method of backing up data of a key-server in communication with a communication network as defined in claim 15 wherein the portable data storage device provides dedicated cryptographic functions for the at least a computer in communication with the communication network using secure electronic key data stored internal to the portable data storage device.

24. (Previously Presented) A method of backing up data of a key-server in communication with a communication network as defined in claim 23 wherein the secure electronic key data stored internal to the portable data storage device are not accessible from outside of the key-server and the portable data storage device.

25. (Previously Presented) A method of backing up data of a key-server in communication with a communication network as defined in claim 15 wherein the key-server provides dedicated cryptographic functions for the at least a computer in communication with the communication network using secure electronic key data stored internal to the key-server.

26. (Previously Presented) A method of backing up data of a key-server in communication with a communication network as defined in claim 25 wherein the secure electronic key data stored internal to the key-server are not accessible in a useable form outside of the key-server and the portable data storage device.

27.-44. (Canceled)

45. (New) A system for storing secure electronic keys, comprising:

a key-server for storing the secure electronic keys, the key-server in communication with a communication network;

a computer in communication with the communication network, the computer having a data reading device for reading data from a portable data storage device; and

a plurality of portable data storage devices each having stored thereon secure electronic key data relating to a single authorized user,

whereby the secure electronic key data relating to the single authorized user is copied from each of the plurality of portable data storage devices for storage in the key-server for restoring or backing up the key data stored in the key-server.

46. (New) A system as defined in claim 45 wherein the key-server has memory means and the key-server and computer form a secure communication session between the key-server and at least one of the plurality of portable data storage devices read by the data reading device and transfer the secure electronic key data via the secure communication session from the portable data storage device to the key-server for storage of the transferred secure electronic key data within the memory means of the key-server.

47. (New) A system as defined in claim 46 wherein the plurality of portable data storage devices includes memory having stored therein all the secure electronic key data to be restored or backed up in the key-server.

48. (New) A system as defined in claim 46 wherein the plurality of portable data storage devices include memory having stored therein secure electronic key data relating to a single authorized user of the communication network.

49. (New) A system as defined in claim 46 wherein at least one portable data storage device includes a processor for ciphering data using the secure electronic key data stored therein by providing cryptographic functions within the portable data storage device using the secure electronic key data stored therein.

50. (New) A system as defined in claim 46 wherein the key-server includes a processor for ciphering data using the secure electronic key data stored therein by providing cryptographic functions within the key-server using the secure electronic key data stored therein.

51. (New) A system as defined in claim 50 wherein the processor is programmed to determine at least an available user information entry device from a plurality of known user information entry devices, to receive unique user identification information via the at least an available user information entry device, and to register the received user identification information against security data for that user stored in the key-server, wherein when the user identification information is indicative of an authorized user the processor ciphers data with secure electronic key data associated with the authorized user.

52. (New) A system as defined in claim 45 wherein the portable data storage device is one of a token and a smart card.

53. (New) A system as defined in claim 46 wherein at least one portable data storage device includes a processor that provides dedicated cryptographic functions for the computer in communication with the communication network using the security data stored internal to the at least one portable data storage device.

54. (New) A system as defined in claim 53 wherein the security data stored internal to the at least one portable data storage device are not accessible in a useable form from outside of the key-server and the at least a portable data storage device.

55. (New) A system as defined in claim 46 wherein the key-server provides dedicated cryptographic functions for the computer in communication with the communication network using the security data stored internal to the key-server.

56. (New) A system for storing secure electronic keys, comprising:

a key-server in communication with a communication network, the key-server having stored therein the unique user identification information for a plurality of authorized users of the communication network and the secure electronic key data for use by the specific authorized user in accessing data within the network;

a computer in communication with the communication network, the computer having a device for reading/writing data from/to a portable data storage device and a device that receives user identification data indicative of an authorized user of the communication network; and

a plurality of portable data storage devices each having stored thereon secure electronic key data relating to a single authorized user, wherein at least one portable data storage device receives from the key-server secure electronic key data relating to the authorized user for use by the specific authorized user in accessing data within the network.

57. (New) A system as defined in claim 56 wherein the at least one portable data storage device has memory means and is assigned to the specific authorized user and the key-server and computer form a secure communication session between the key-server and the at least one portable data storage device read by the data reading/writing device and transfer the secure electronic key data relating to the specific authorized user via the secure communication session from the key-server to the at least one portable data storage device for storage of the transferred secure electronic key data within the memory means of the at least one portable data storage device.

58. (New) A system as defined in claim 57 wherein secure electronic key data specific to each of a plurality of authorized users of the communication network is stored on a separate portable data storage device assigned uniquely to one of the plurality of authorized users, wherein the secure electronic key data of the key-server is partially stored within each portable data storage device and wherein all data within the plurality of portable data storage devices is sufficient to restore security data to the key-server in the event of a data loss thereto.

59. (New) A system as defined in claim 56 wherein the portable data storage device includes a processor for ciphering data using the secure electronic key data stored therein by providing cryptographic functions within the portable data storage device using the secure electronic key data stored therein.

60. (New) A system as defined in claim 56 wherein the key-server includes a processor for ciphering data using the secure electronic key data stored therein by providing cryptographic functions within the key-server using the secure electronic key data stored therein.

61. (New) A system as defined in claim 60 wherein the processor is programmed to determine at least an available user information entry device from a plurality of known user information entry devices, to receive unique user identification information via the at least an available user information entry device, and to register the received user identification information against security data for that user stored in the key-server, wherein when the user identification information is indicative of an authorized user the processor ciphers data with secure electronic key data associated with the authorized user.

62. (New) A system as defined in claim 56 wherein at least one portable storage device comprises an interface.

63. (New) A system as defined in claim 57 wherein the at least one portable data storage device provides dedicated cryptographic functions for the computer in communication with the communication network using secure electronic key data stored internal to the at least one portable data storage device.

64. (New) A system as defined in claim 63 wherein the secure electronic key data stored internal to the at least one portable data storage device are not accessible from outside of the key-server and the at least one portable data storage device.

65. (New) A system as defined in claim 57 wherein the key-server provides dedicated cryptographic functions for the computer in communication with the communication network using secure electronic key data stored internal to the key-server.

66. (New) A system as defined in claim 65 wherein the secure electronic key data stored internal to the key-server are not accessible in a useable form outside of the key-server and the at least one portable data storage device.